ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Laboratorio di

Sicurezza Informatica

Esercitazioni: GPG

Andrea Melis
Marco Prandini
Dipartimento di Informatica – Scienza e Ingegneria

Creare una chiave GPG

- **Utility gpg**

```
gpg --gen-key
Selezionare identità
Grandezza chiave (>= 2048)
Data di Scadenza! (importante)
Passphrase
```

Gestione Chiave

- A questo punto potete importate ed esportare vostre chiavi o di un altra identità
- Prima di tutto però, dove si trovano le chiavi?
- Cartella .gnupg/ della vostra home page

```
cd ~
cd .gnupg/
ls -l
Chiavi pubbliche in : pubring.kbx
Chiavi private in : directory private-keys.d/ con estensione .key
Potete scegliere la vostra configurazione in: gpg.conf
```

Importare Chiave

- **Potete importare la chiave sia con copy/paste da terminale sia importare il file direttamente.**

```
gpg --import
Incollare la chiave pubblice
gpg --import vostrachiavepubblica.pub
Importando la chiave vi verrà stampato il Key-ID
gpg --list-keys Key-ID
Visualizzazione chiave importate ( senza Key-ID le
visualizza tutte)
```

Esportare Chiave Privata

- In teoria potete esportare la vostra chiave con:

```
gpg --output private.pgp --armor --export-secret-key
vostraidentita@email
```

- Tuttavia è fortemente sconsigliato esporta la propria chiave privata. Non ci sono delle situazione dove sia strettamente necessario e non deve ovviamente MAI essere distribuita.

- L'unica situazione che può richiederlo è quando avete bisogno di un backup della chiave privata, in quel caso potete usare l'utility backup

```
gpg --output backupkeys.pgp --armor --export-secret-
keys --export-options export-backup
vostraidentita@email
```

Esportare Chiave Pubblica

- **Esportare una chiave pubblica:**

```
gpg --output public.pgp --armor --export identita@email
```

GPG vs PGP

- PGP è l'acronimo di Pretty Good Privacy. È stato creato negli anni '90 ed è attualmente di proprietà della società di software di sicurezza Symantec. Nel corso di quasi tre decenni, PGP è stato sviluppato, migliorato e aggiornato, rendendolo oggi l'opzione standard per la crittografia dei file.

- PG, o GnuPG, sta per GNU Privacy Guard. GPG è un'implementazione diversa dello standard Open PGP e una valida alternativa al software PGP ufficiale di Symantec. GPG è definito da RFC 4880. GPG può aprire e decrittografare i file crittografati da PGP o Open PGP, il che significa che funziona bene con altri prodotti.

GPG vs PGP

- PGP è una soluzione proprietaria, di proprietà di Symantec e GPG (noto anche come GnuPG) è uno standard open source. Funzionalmente, ogni formato è praticamente identico.

PGP Mit Key Server

- Server dove è possibile pubblicare le proprie chiavi pubbliche.

- Come? Recuperiamo prima il Key-ID della nostra chiave

```
gpg --keyid-format LONG --list-keys a.melis@unibo.it
pub   rsa2048/9D6A4A7849845D01 2018-04-01 [SC]
[expires: 2023-03-31]
      AD54A494EF4F97AF54E9FDC59D6A4A7849845D01
uid           [ unknown] Andrea Melis <a.melis@unibo.it>

gpg --keyserver pgp.mit.edu -send-keys 9D6A4A7849845D01
```

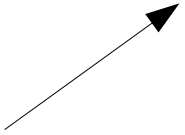
Server PGP Mit (Alternativo keys.openpgp.org)

PGP Mit Key Server

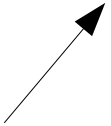
- Allo stesso modo è possibile recuperare le chiavi pubbliche del nostro target, come?

- Una volta recuperato dal server attraverso una semplice richiesta per utente (tipicamente una mail), l'ID della identità per la quale vogliamo scaricare la chiave possiamo fare:

```
gpg --keyserver pgp.mit.edu --recv-keys 49845D01
```



Server PGP Mit



a.melis@unibo.it ID

PGP Key Server Alternativi

- hkp://keyserver.ubuntu.com

- hkp://keys.gnupg.net

Cifrare

- Cifrare un file con una chiave pubblica è abbastanza semplice

```
gpg --encrypt --armor -r identita@mail file_da_crittare
```

- Con opzione -r potete crittare con più chiavi

Cifrare e Firmare

- Cifrare e firmare un file è sufficente aggiungere -sign

```
gpg --encrypt --armor --sign -r identita@mail
file_da_crittare
```

Decifrare

- Decifrare un file con la vostra chiave privata è abbastanza semplice

```
gpg --decrypt  file_da_crittare
```

Firmare una chiave

- Potete firmare la chiave pubblica di qualcuno.

```
gpg --sign-key identita@mail
```